

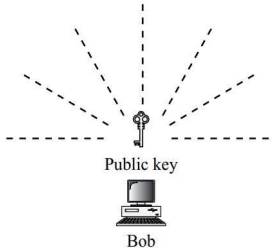
Shiv Nadar University Chennai

End Semester Examinations, 2023-2024 Even

Question Paper

Name of the Program: B.Tech. CSE (Cyber Security)	Semester: II
Course Code & Name: CS1008 Classical Cryptography	
Regulation 2021	
Time: 3 Hours	Maximum: 100 Marks

Answer any 10 Questions.

Q.No.		Questions	Marks	CO#	KL#	
1	a	Differentiate symmetric and asymmetric encryption focusing on nature of the keys, working principle, and context in which they are used. Distinguish with an example.	5	CO1	KL4	
	b	Explain Fermat’s and Euler’s theorems with examples.	5	CO2	KL2	
2	a	Engineers are developing a secure communication protocol for transmitting sensitive data over a network in a cyber security firm. They plan to implement asymmetric encryption and are given two numbers 1971, and 1067. What is the relationship between the two numbers? Show with an algorithm that the relationship holds for the two numbers and calculate the time complexity of the algorithm.	10	CO2	KL3	
3	a	Write down the alphabet to numeric mapping for encoding alphabets into numbers. Apply Vignere cipher for the given sentence “TO BE OR NOT TO BE” with the key “CODE”.	4	CO1	KL3	
	b	With the Caesar and Substitution ciphers we can use frequency analysis to guess some of the letters in the cipher text. Can we use frequency analysis with the Vignere cipher? Explain objectively with numeric examples.	6	CO1	KL2	
4	a	What is a cryptographic hash function and what is it used for? If you use a poor hash function, mention three potential problems that she would have to face? Explain each scenario with an example.	10	CO3	KL2	
5	a	Give the architectural diagram for MDC and MAC. What security service does each of them provide? Explain. Describe a scenario where both an MDC and a MAC are utilized in a secure communication environment.	10	CO3	KL3	
6	a	Let’s say Indraneel and Saharu decide on communicating with each using the RSA algorithm. Saharu needs to send a message $m = 8$ to Indraneel. Who should generate the public and private key? What is the private and public key pair if $p=7$; $q=11$; $e=17$? Give the encryption and decryption process for the mentioned scenario. Why is RSA tough to calculate?	10	CO4	KL3	
7	a	What is the need for key management? Why do you need a separate key management strategy for private and public key cryptography? Why is the given scenario not ideal for distributing public keys? Explain in detail two ways in which private keys can be distributed.		10	CO4	KL2
8	a	What is the main idea behind Feistel rounds? Draw the Feistel structure of Blowfish. How is it different from the regular Feistel rounds? Explain the role of each part of Blowfish.		10	CO3	KL2
9	a	List and describe the general two types of attacks and their sub-classifications.	10	CO5	KL2	

		Consider the web application-health care domain. Using these sub-classifications, what real-world attacks are possible on the web-application? What can the attacker gain from each attack? List down any 8 such attacks and describe them briefly.			
10	a	What is an elliptic curve? Explain with a clear diagram explaining how the elliptic curve cryptography utilizes the properties of an elliptic curve for improved security?	5	CO4	KL2
	b	What security service does a digital signature offer? Explain with a diagram the process of digital signatures in the scenario where Indraneel signs a message and sends it to Saharu.	5	CO4	KL2

KL – Bloom's Taxonomy Levels

(KL1: Remembering, KL2: Understanding, KL3: Applying, KL4: Analyzing, KL5: Evaluating, KL6: Creating)

CO – Course Outcomes
